# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-244483
(43)Date of publication of application : 08.09.2000

(51)Int.CI. H04L 9/32
G06F 13/00
G06F 17/60
H04L 9/08
H04L 12/54
H04L 12/58

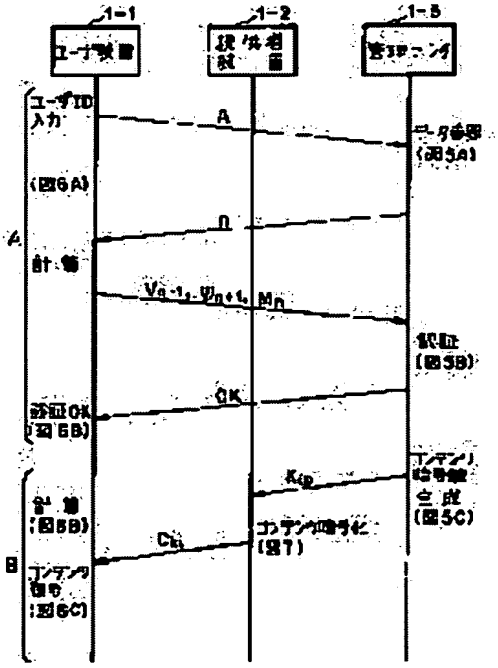
(21)Application number : 11-044271
(22)Date of filing : 23.02.1999

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : HORIOKA TSUTOMU
SONEHARA NOBORU
KAWAMURA TORU
TSURUMAKI KOJI



## (54) METHOD AND DEVICE FOR CONTENT DELIVERY, METHOD AND DEVICE FOR RECEPTION, AND PROGRAM RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To safely and securely deliver a content ciphering key by setting a one time password used in a user authentication procedure as a parameter, independently calculating the content ciphering key on a user side and a content supply side with a unidirectional function and generating the same key.
SOLUTION: The same key is generated by independently calculating a content ciphering key on a user side and a content supply side without transmitting it to an opposite party through communication by a unidirectional function with a one time password used in a user authentication procedure as a parameter. In the system, the device 1-1 of a user buying a content and the device 1-2 of a supplier selling the content are connected to a channel. The device 1-2 of the content supplier is connected with a management center 1-3 by the channel. The management center 1-3 executes authentication and accumulates/ manages various data for the device 1-1 of the user or the device 1-2 of the supplier.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－244483
（Ｐ2000－244483Ａ）
(43)公開日　平成12年９月８日(2000.9.8)

| (51)Int.Cl.' | 識別記号 | ＦＩ | | テーマコード'(参考) |
|---|---|---|---|---|
| Ｈ04Ｌ　9/32 | | Ｈ04Ｌ　9/00 | 673Ａ | 5Ｂ049 |
| Ｇ06Ｆ　13/00 | 354 | Ｇ06Ｆ　13/00 | 354Ｚ | 5Ｂ089 |
| 17/60 | | 15/21 | 330 | 5Ｊ104 |
| Ｈ04Ｌ　9/08 | | Ｈ04Ｌ　9/00 | 601Ｄ | 5Ｋ030 |
| 12/54 | | | 601Ｅ | |

審査請求　未請求　請求項の数６　ＯＬ　（全９頁）　最終頁に続く

(21)出願番号　特願平11－44271

(22)出願日　平成11年２月23日(1999.2.23)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号

(72)発明者　堀岡　力
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　曽根原　登
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　100066153
弁理士　草野　卓　（外１名）

最終頁に続く

(54)【発明の名称】　コンテンツ配送方法、受信方法、コンテンツ配送装置、受信装置、およびそれらのプログラム記録媒体

(57)【要約】
【課題】　コンテンツ暗号化用鍵Ｋｉを、ユーザ側、コンテンツ提供側のそれぞれで独立に計算可能とする。
【解決手段】　ユーザＵはパスワードＳとユーザＩＤＡとを用いて計算したワンタイムパスワード$W_0$、$W_1$、$M_0$とＡをセンタに登録し、センタは認証回数ｎを０とし、センタはＵからコンテンツ配送要求が来ると、ｎを更新してＵへ送り、Ｕは$V_{n-1}=E(A, S(+)(n-1))$、$W_{n+1}=E(A, V_{n+1})$、$M_n=E(V_n, W_{n+1})$（Ｅは一方向性関数）を計算してセンタへ送る。センタは$W_{n-1}=E(A, V_{n-1})$を計算し、これと登録した$W_{n-1}$と比較し、一致すれば$M_{n-1}=E(W_n, V_{n-1})$を計算し、登録した$M_{n-1}$と比較し、一致すれば$W_n$、$M_{n-1}$が正しいと判断し、Ｖに認証ＯＫを送る。Ｕの秘密鍵Ｓ、を用いＫｉ＝Ｅ（$S_n$、$M_{n-1}$）を求める。Ｕは$V_n=E(A, S(+)n)$、$W_n=E(A, V_n)$、$M_{n-1}=E(W_n, V_{n-1})$を順次計算し、Ｋｉ＝Ｅ（$M_{n-1}$、$S_n$）を求める。

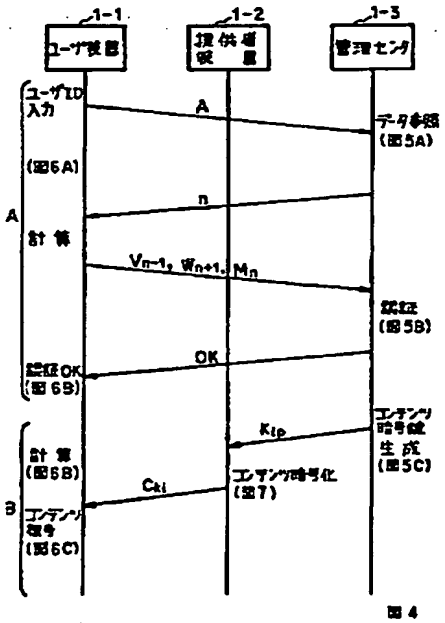



図４

1

【特許請求の範囲】
【請求項１】 通信回線を通じてユーザ装置からコンテンツデータ配送要求を受信する手段と、
前記通信回線を通じて前記ユーザ装置から毎回異なる認証データを受信する手段と、
前記認証データに対し、前記ユーザ装置認証のための検証処理をする手段と、
前記認証データに基づいて暗号化鍵を生成する手段と、
前記暗号化鍵を用いて前記要求されたコンテンツデータを暗号化する手段と、
前記暗号化コンテンツデータを前記通信回線を通じて配送する手段と、
を有するコンテンツデータ配送装置。
【請求項２】 通信回線を通じてコンテンツデータ配送要求を送信する手段と、
前記配送要求を送信ごとに、毎回異なる認証データを生成する手段と、
前記通信回線を通じて前記認証データを、前記コンテンツデータ配送要求送信先に送信する手段と、
前記認証データを用いて復号鍵を生成する手段と、
暗号化されたコンテンツデータを受信する手段と、
前記復号鍵を用いて前記暗号化されたコンテンツデータを復号する手段と、
を有するコンテンツデータ受信装置。
【請求項３】 通信回線を通じてユーザ装置からコンテンツデータ配送要求を受信する過程と、
前記通信回線を通じて前記ユーザ装置から毎回異なる認証データを受信する過程と、
前記認証データに対し、前記ユーザ装置認証のための検証処理をする過程と、
前記認証データに基づいて暗号化鍵を生成する過程と、
前記暗号化鍵を用いて前記要求されたコンテンツデータを暗号化する過程と、
前記暗号化コンテンツデータを前記通信回線を通じて配送する過程と、
を有するコンテンツデータ配送方法。
【請求項４】 通信回線を通じてコンテンツデータ配送要求を送信する過程と、
前記配送要求を送信ごとに、毎回異なる認証データを生成する過程と、
前記通信回線を通じて前記認証データを、前記コンテンツデータ配送要求送信先に送信する手段と、
前記認証データを用いて復号鍵を生成する過程と、
暗号化されたコンテンツデータを受信する過程と、
前記復号鍵を用いて前記暗号化されたコンテンツデータを復号する過程と、
を有するコンテンツデータ受信方法。
【請求項５】 通信回線を通じてユーザ装置からコンテンツデータ配送要求を受信する処理と、
前記通信回線を通じて前記ユーザ装置から毎回異なる認証データを受信する処理と、
前記認証データに対し、前記ユーザ装置認証のための検証処理をする処理と、
前記認証データに基づいて暗号化鍵を生成する処理と、
前記暗号化鍵を用いて前記要求されたコンテンツデータを暗号化する処理と、
前記暗号化コンテンツデータを前記通信回線を通じて配送する処理と、
をコンテンツデータ配送装置のコンピュータに実行させるプログラムを記憶した記録媒体。
【請求項６】 通信回線を通じてコンテンツデータ配送要求を送信する処理と、
前記配送要求を送信ごとに、毎回異なる認証データを生成する処理と、
前記通信回線を通じて前記認証データを、前記コンテンツデータ配送要求送信先に送信する処理と、
前記認証データを用いて復号鍵を生成する処理と、
暗号化されたコンテンツデータを受信する処理と、
前記復号鍵を用いて前記暗号化されたコンテンツデータを復号する処理と、
をコンテンツデータ受信装置のコンピュータに実行させるプログラムを記憶した記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、例えば通信を利用したオンラインショッピングにおいて、情報等のコンテンツを安全かつ正しく購入するためのコンテンツ配送、受信方法とそれに用いる装置およびそのプログラムを記録した記録媒体に関するものである。
【０００２】
【従来の技術】インターネット等の広域コンピュータネットワークにおいて、コンピュータを通信によって結合してコンテンツを売買する商取引形態では、一般的な対面販売に比べ、相手がコンテンツを受け取る資格を有する者か否かの検証と、コンテンツの内容が途中で改鼠（かいざん）等されることなく正しく届けられること、の仕組みがより重要である。
【０００３】このためにコンテンツ売買の手順としては、はじめにコンテンツを受け取る資格を有する者か否かを確認する“ユーザ認証”を行い、確認できた後に、コンテンツが途中で改鼠等されずに正しい内容で届くよう、また資格のない第三者が不当に入手することのないように“コンテンツを暗号化”して相手に送付し、コンテンツ購入者は、別途入手した暗号化用鍵でコンテンツを復号化することが一般的である。
【０００４】コンテンツの暗号化では、より安全に行えるよう種々の提案がなされている。例えば、Ｋｅｒｂｅｒｏｓは、暗号化のために長い間同じ鍵が使用されると、鍵が解読される危険性が高くなることを回避するため、指定された期間内のみ有効な鍵を使用する方法を提

案している。しかし、この方法でもコンテンツの復号化のためにユーザへ鍵を送付することが必要であり、また管理センタとコンテンツ提供者が異なる場合は、コンテンツ暗号化用鍵をコンテンツ提供者へ送付するという手順そのものが必要であり、またネットワークの全てのユーザの端末で時間が一致した時計を持つことが必要である。

【０００５】また、上記のユーザ認証やコンテンツの暗号化では、従来の方法はＩＣカードを利用したり、乱数発生や高度な計算処理を必要としていた。このため各ユーザが使用する端末において、ＩＣカード用リードライト機能や高度な制御動作を必要とし、端末の低価格化に限界があった。

【０００６】

【発明が解決しようとする課題】このため、より安全・確実な方法でかつ端末への負担が少なく、安価な端末でも実現できるコンテンツ暗号化用鍵の配送方法が望まれていた。この発明は、上記問題点を解決するためになされたもので、コンテンツ暗号化用鍵をより安全・確実に配送でき、さらにユーザの装置に対して計算処理の負担や時計に対する負担が小さいコンテンツ暗号化用鍵の配送方法ならびにそれに使用する装置およびそのプログラムを記録した記録媒体の提供を目的とするものである。

【０００７】

【課題を解決するための手段】この発明は、上記課題を実現するために以下のような構成としたことを特徴とする。コンテンツ配送に先立ち、ユーザとコンテンツ提供側との間でユーザ認証の手順を行う方法において、ユーザ認証手順で使用したワンタイムパスワード（照合の都度、変化する認証データ）をパラメータとして、一方向性関数によりコンテンツ暗号化用鍵を、通信により相手に送信することなく、ユーザ側とコンテンツ提供側とでそれぞれ独立に計算することにより同一の鍵を生成する。しかもコンテンツ暗号化用鍵の生成において、ＩＣカードを利用したり、高度の計算処理なしに生成できるようにしたものである。

【０００８】

【発明の実施の形態】図１は、この発明を説明するためのシステム構成図で、図１Ａにおいて、コンテンツを購入するユーザの装置１－１と、コンテンツを販売する提供者の装置１－２は通信路で結合される。コンテンツ提供者装置１－２は管理センタ１－３と通信路で結合されている。管理センタ１－３はユーザ装置１－１または提供者装置１－２との間での認証や種々のデータ蓄積・管理を行う機関である。ユーザ装置１－１、提供者装置１－２および管理センタ１－３には、それぞれ情報の送受、データ蓄積ならびに計算を行うことのできる機能とその制御プログラムが備えられている。

【０００９】また規模が小さい場合は、図１Ｂに示すように、コンテンツ提供者装置１－２と管理センタ１－３とが一体化した構成もある。この発明では、コンテンツ提供者装置と管理センタ（コンテンツ提供者装置１－２と管理センタ１－３を一体化した場合と分離した場合とを含む）をコンテンツ提供側と記述する。なお、以下の説明では図１Ａの構成について説明する。

【００１０】この他、売買代金を決済する決済機関も必要であるが、この発明では直接関係しないので記述は省略してある。

（１）事前登録

図１Ａの構成で、コンテンツの送受を安全に行うために、実際のコンテンツ送受に先立ち事前の登録が必要であるから、はじめにこれについて説明する。

【００１１】図２は、ユーザを管理センタへ登録する手順を説明した図である。はじめにユーザ装置１－１が、入会申請として、決済用の口座番号等の送付を管理センタ１－３に対して行う。管理センタ１－３は、ユーザ登録を行いユーザＩＤ（識別情報）としてＡをユーザ装置１－１へ返送する。ユーザ装置１－１では、Ａとユーザ自身が定めた任意のパスワードＳとを用いて、３つのワンタイムパスワード$W_0$，$W_1$，$M_0$を計算する。この計算は$V_0$＝Ｅ（Ａ、Ｓ），$W_0$＝Ｅ（Ａ、$V_0$）．$V_1$＝Ｅ（Ａ、Ｓ（＋）１），$W_1$＝Ｅ（Ａ、$V_1$）．$M_0$＝Ｅ（$W_1$、$V_0$）（Ｅは一方向性関数、（＋）はビットごとの排他的論理和をそれぞれ表わす）を順次計算して求める。ワンタイムパスワードの計算は、次項（２）の“ユーザ認証”の手順と同一であるので、次項で詳述する。計算したワンタイムパスワード$W_0$，$W_1$，$M_0$を管理センタ１－３へ送付する。

【００１２】管理センタ１－３では、ユーザ登録としてユーザＩＤ　Ａ、認証回数ｎの初期値としてｎ＝０およびユーザ装置１－１より送られた$W_0$，$W_1$，$M_0$、さらにユーザ装置１－１に固有の秘密鍵$S_0$を生成し、これらをセットにしてそのユーザの初期登録データとして蓄積・管理する。管理センタ１－３は、秘密鍵$S_0$をユーザ装置１－１へ送付する。ユーザ装置１－１では、秘密鍵$S_0$、ユーザＩＤＡ、パスワードＳを秘密にし蓄積・管理する。

【００１３】図３は、コンテンツ提供者を管理センタへ登録する手順を説明する図である。はじめに提供者装置１－２は、契約申込みとして、決済用の口座番号等の申込みを管理センタ１－３に対して行う。管理センタ１－３は、提供者登録を行うと共に提供者装置１－２に固有の秘密鍵Ｓｐを生成し、蓄積・管理すると共に、提供者装置１－２に送付する。提供者装置１－２は、Ｓｐを秘密にし蓄積・管理する。

【００１４】図２および図３での情報の送受は、初期登録として１回行われればよく、必ずしも通信である必要はなく郵送等でもよい。また、秘密鍵$S_0$、ユーザＩＤＡ、および、パスワードＳ決定は、ユーザ装置において決定することも可能であることは言うまでもない。

（2）ユーザ認証

オンラインでのユーザ認証およびコンテンツ配送の手順を図4に示す。図4は、ユーザ装置、提供者装置、管理センタ間の情報送受の流れを記述したもので、さらに管理センタにおける制御動作を図5に、ユーザでの制御動作を図6に、提供者装置での制御動作を図7に、それぞれ示してある。はじめに、ユーザ認証について説明する。（図4A）

コンテンツを購入しようとするユーザ装置1－1は、ユーザID Aを管理センタ1－3へ送信する。

【0015】管理センタ1－3は、図5Aに示すように、受信したユーザID Aが既に登録済みであるか否＊かをチェックする（S1）。登録済みであれば、図2に示した登録済みのAのデータを参照すると共に（S2）、認証回数nの登録値に＋1した値nをユーザ装置1－1へ返送する（S3）。ただし、登録値を予め＋1しておくことにより、登録値をそのまま返送することも可能である。

【0016】ユーザ装置1－1では、図6Aに示すように管理センタ1－3からnを受信したら（S2）、3つのワンタイムパスワード$V_{n-1}$、$W_{n-1}$、および$M_n$をパスワードSとID Aから計算する（S3）。3つのワンタイムパスワードは、それぞれ以下に示す式（1）、式（2）、式（3）で計算される。

$$V_{n-1}=E(A, S(+)(n-1)) \quad (1)$$

$$W_{n-1}=E(A, V_{n-1}) \quad (2)$$

$$M_n=E(V_n, W_{n-1}) \quad (3)$$

ただし、Eは一方向性関数、（＋）は排他的論理和

$V_{n-1}$は、登録されているユーザID Aと、パスワードSと管理センタ1－3から受信したnから1を引いた値との排他的論理和とをパラメータとして、一方向性関数により計算された今回の被認証データである。$W_{n-1}$は、ユーザIDAと、式（1）においてn－1をn＋1として求めた$V_{n-1}$とをパラメータとして、一方向性関数により計算された次々回認証データである。$M_n$は、式（2）において求められた$W_{n-1}$と式（1）において、n－1をnとして求めた$V_n$とをパラメータとし※て、一方向性関数により計算された次々回認証データ$W_{n-1}$の正当性検証データである。$V_{n-1}$、$W_{n-1}$、$M_n$の全体を認証データと呼ぶこともある。

$$W_{n-1}=E(A, V_{n-1}) \quad (4)$$

を計算し（S5）、既に管理センタ1－3に登録されている、このユーザ装置1－1の$W_{n-1}$と比較する（S6）。一致した場合は、ユーザ装置1－1から送られた$V_{n-1}$が正しいことが証明されたので、管理センタ1－★3ではユーザの認証後、既に登録されているユーザの秘密鍵S。とユーザ認証手順で正しいことが証明された$M_{n-1}$とをパラメータとして式（6）に示す一方向性関数により、

$$M_{n-1}=E(W_n, V_{n-1}) \quad (5)$$

$M_{n-1}$を計算し（S7）、既に管理センタ1－3に登録されている$M_{n-1}$と比較する（S8）。正しいことが証明された$V_{n-1}$と正しいか否か不明の$W_n$をパラメータとして式（5）により計算した$M_{n-1}$は、1つしか存在しないから、これが登録されている$M_{n-1}$と一致すれば、管理センタ1－3で既に預かっていた$W_n$は正しく、同時に$M_{n-1}$も正しいことが証明されるので、管理センタ1－3ではユーザ装置1－1に対して認証OKを送信すると共に（S9）、預かっているデータn、$W_n$、$W_{n-1}$、$M_n$を更新する（S10）。

【0018】以上説明したユーザ認証の手順は、特願平09－247133に記述されている方法と同様である。図4では、情報の送受は、ユーザ装置1－1と管理センタ1－3間で直接行う場合について説明したが、提供者装置1－2を介して行ってもよいことは無論である。

【0019】次にコンテンツの配送について説明する。

（3）コンテンツの配送

① コンテンツ暗号化用鍵の生成

★3では$V_{n-1}$と既に管理センタ1－3に登録されている$W_n$とをパラメータとして式（5）に示す一方向性関数により、

$$K_i=E(S_c, M_{n-1}) \quad (6)$$

コンテンツ暗号化用鍵$K_i$を生成する。

【0020】次いで管理センタ1－3は鍵$K_i$と既に登録されている提供者装置の秘密鍵$S_p$とをパラメータとして式（7）に示す一方向性関数により、

$$K_{ip}=E(K_i, S_p) \quad (7)$$

鍵$K_i$を鍵$S_p$で暗号化して（S11）、提供者装置1－2へ送信する（S12）。

【0021】ここで重要なことは、この発明によれば、コンテンツ暗号化用鍵$K_i$は、管理センタ1－3からユーザ装置1－1には送信されず、ユーザ装置1－1では$K_i$を自分自身で計算により生成できるということである。すなわちユーザ装置1－1では、ユーザ認証で管理センタ1－3から認証OKを受信した後は（S5）、図

6Bに示すように、ユーザＩＤ Aと、パスワードSおよびnの排他的論理和とをパラメータとして、式（8）に示す一方向性関数によりV。を計算する。

【0022】

$V_0 = E(A, S(+)n)$ （8）

次に、ユーザＩＤ Aと式（8）で計算されたV。とから、式（9）に示す一方向性関数によりW。を計算する。

$W_0 = E(A, V_0)$ （9）

さらに、式（9）で計算されたW。とユーザ認証で計算されたV$_{n-1}$とから、式（10）に示す一方向性関数によりM$_{n-1}$を計算する（S6）。

【0023】

$M_{n-1} = E(W_0, V_{n-1})$ （10）

M$_{n-1}$と既に所有している秘密鍵S。とから式（11）に示す一方向性関数により、

$Ki = E(M_{n-1}, S_0)$ （11）

Kiを自分自身で計算する（S7）。式（11）は式（6）と同一であり、管理センタ1－3で生成した鍵Kiを、ユーザ装置1－1自身でも生成することができる。

【0024】② コンテンツの暗号化

図4Bおよび図7に示すように、管理センタ1－3よりKipを受信した提供者装置1－2は、式（12）に示す一方向性関数によりKiを入手する（S1）。

$Ki = E(Kip, Sp)$ （12）

次いで提供者装置1－2は、コンテンツ暗号化用鍵Kiを用いてコンテンツCを式（13）に示す一方向性関数により暗号化し、暗号化されたCkiをユーザへ送信する（S2）。

【0025】

$Cki = E(C, Ki)$ （13）

Kiにより暗号化されたコンテンツを受信したユーザ装置1－1は、前記（3）①項で説明したように式（11）により自分自身で計算した鍵Kiを用いて式（14）に示す一方向性関数により、コンテンツCkiを復号化して、コンテンツCを入手する（S8）。

【0026】

$C = E(Cki, Ki)$ （14）

このようにして、コンテンツ復号化のための鍵をユーザ装置1－1へ送ることなしに、ユーザ装置1－1は暗号化されたコンテンツから元のコンテンツを安全に入手することができる。上述ではコンテンツ暗号化用鍵の生成にM$_{n-1}$を用いたが、送ったデータが正しいことが証明されているものであれば他のもの、つまりW$_{n-1}$、W。、V$_{n-1}$の何れかを用いてもよい。

【0027】（4）装置構成

図8は、この発明を実施するための装置の機能構成の一実施例で、ユーザ装置1－1および提供者装置1－2で使用する装置、および管理センタ1－3で使用する制御装置において利用される。ここでは、ユーザ装置1－1または管理センタ1－3での利用を中心に説明する。

【0028】通信制御手段8－1は、通信相手である管理センタ1－3またはユーザ装置1－1との間で情報を送受するための手段で、接続される回線に適合する電気・物理条件ならびに通信プロトコルを備えている。バッファ手段8－2は通信相手である管理センタ1－3またはユーザ装置1－1との間で情報を送受するとき、受信した情報を装置内で処理するために一時的に蓄積したり、装置内で処理し相手に送信する情報を一時的に蓄積するための手段である。

【0029】データ蓄積手段8－3は、管理センタ1－3では図2に示したユーザデータであるA、n、V。、W$_{n-1}$、M。、S。等を、またユーザ装置1－1では、A、S。等を蓄積しておく手段である。計算手段8－4はユーザ装置1－1では、前述した式（1）～式（3）、式（8）～式（11）、式（14）、管理センタ1－3では式（4）～式（7）にそれぞれ示した計算を行うための手段である。

【0030】比較手段8－5は、計算手段8－4で計算した結果とデータ蓄積手段8－3内のデータとを比較したり、受信してバッファ手段8－2に蓄えられたデータと、データ蓄積手段8－3のデータとを比較したり等を行う手段である。入力手段8－6は、ユーザ装置1－1ではパスワードSの入力の他、ユーザＩＤの入力やコンテンツ購入等の意志を伝えるための手段、また管理センタ1－3では、データ蓄積手段8－3へ、ユーザ装置1－1や提供者装置1－2の情報を入力したり、オペレータの操作等を行うための手段である。

【0031】表示手段8－7は、入力手段8－6で入力するときの入力確認や、比較手段8－5での比較結果や通信の状況をユーザまたは管理センタのオペレータに伝えるための手段である。制御手段8－8は、図5または図6に示す制御動作ならびに装置全体の制御を行う手段である。

【0032】

【発明の効果】以上説明したように、この発明によれば、ユーザ認証の手順で生成したパラメータをコンテンツ暗号化用鍵の生成に流用し、コンテンツ提供側およびユーザ装置自身で、それぞれ独立して計算によりコンテンツ暗号化用の鍵を生成できるので、ユーザ装置に対するコンテンツ暗号化用鍵の配送を省略することができ、かつ暗号化に使われる鍵は毎回変わるので、きわめて安全性の高い鍵の配送を確実に行うことができる。

【0033】また、ユーザ認証で行う計算処理、使用するパラメータは、特願平09－247133にも示すようにＩＣカード等の記憶媒体の読み書きを行う機能や乱数発生や高度な計算処理機能を必要としないので、この手順を一部流用するこの発明においても、被認証側にＩＣカード等の記憶媒体の読み書きを行う機能や乱数発生

や高度の計算処理機能を必要としないので、小さいプログラムサイズでの処理が可能である。このため処理能力の限られた安価な装置を使用することができ、安全なコンテンツ売買を経済的に実現することが可能である。

【図面の簡単な説明】

【図１】この発明を説明するためのシステム構成を示す図。

【図２】ユーザを管理センタに登録する手順例の説明図。



＊【図３】コンテンツ提供者を管理センタへ登録する手順例の説明図。

【図４】ユーザ認証およびコンテンツ配送の手順例の説明図。

【図５】管理センタ装置の制御動作例の説明図。

【図６】ユーザ装置の制御動作例の説明図。

【図７】コンテンツ提供者装置の制御動作例の説明図。

【図８】この発明を実施する装置の構成例を示す図。

＊

【図１】

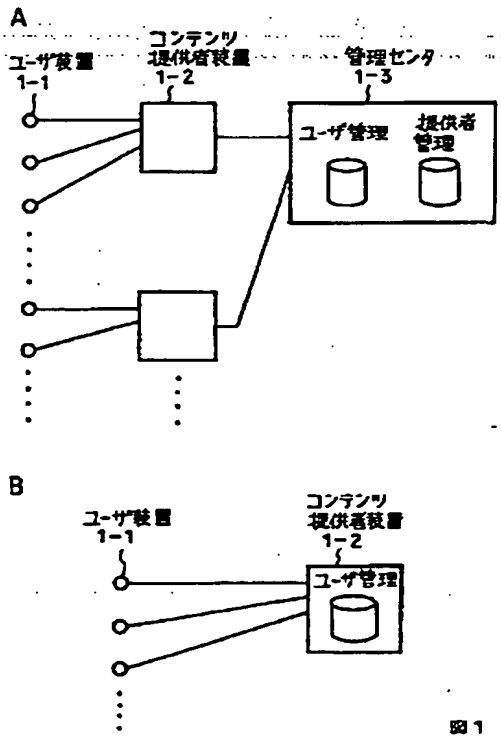



図１

【図２】

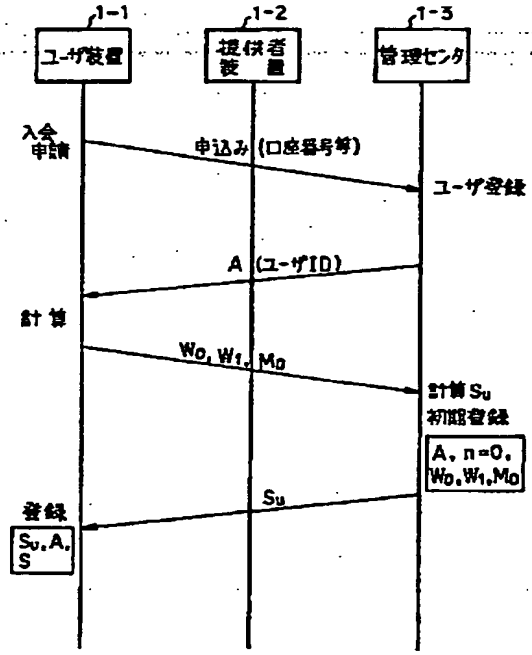



図２

【図3】

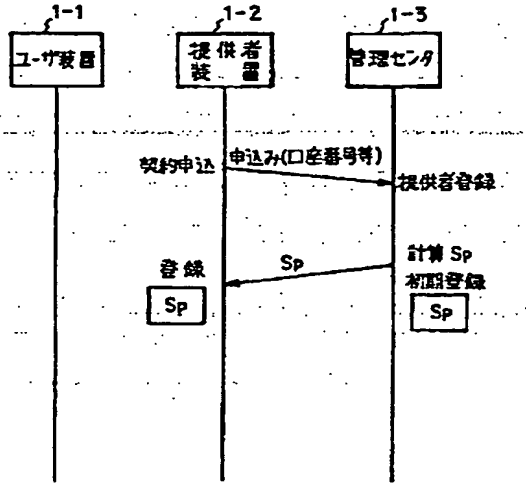



図3

【図4】

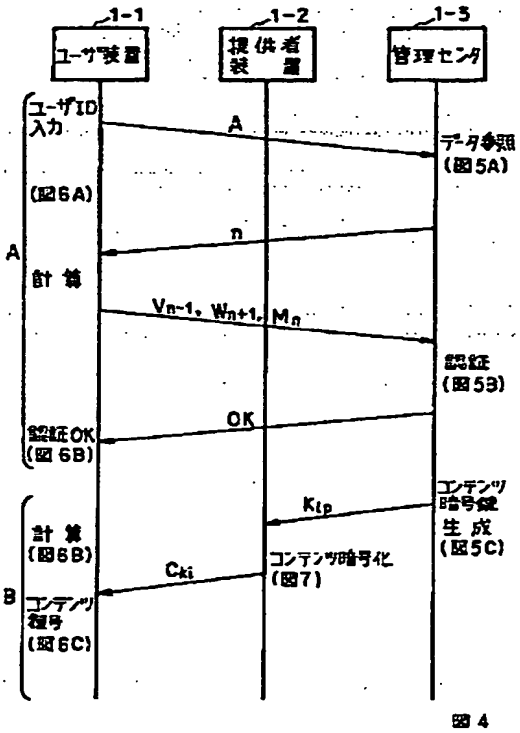



図4

【図7】

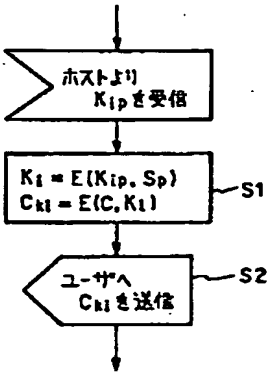



図7

【図5】

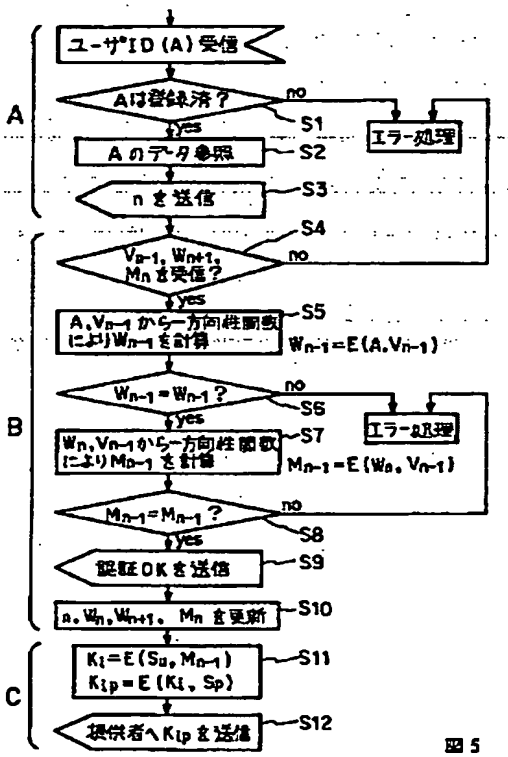



図5

【図6】

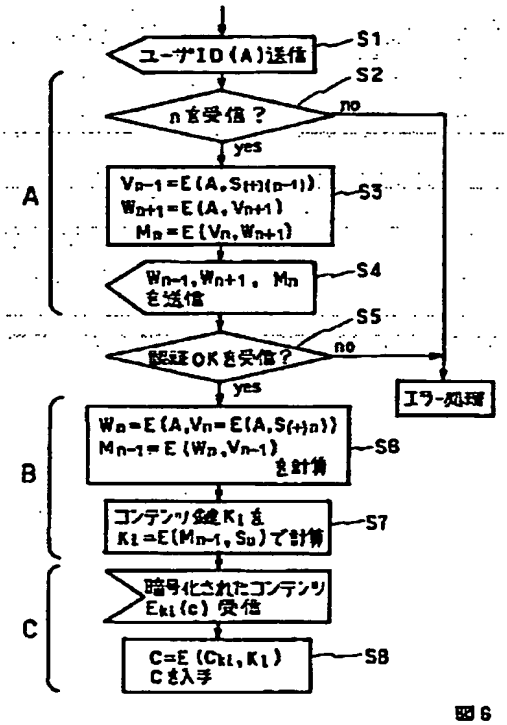



図6

【図8】

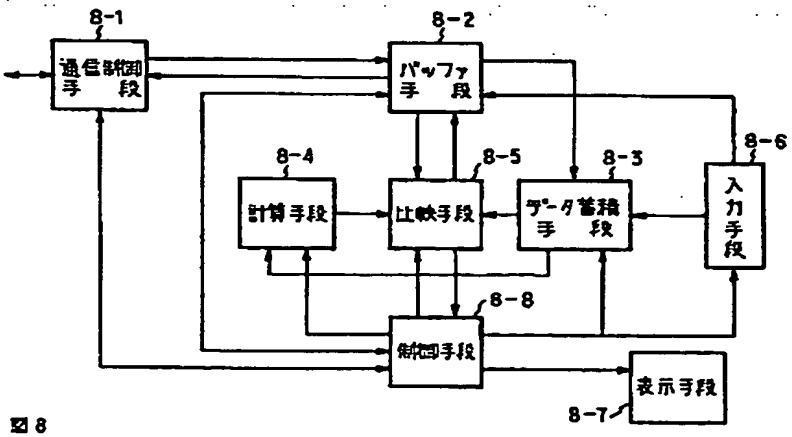



図8

フロントページの続き

| (51)Int.Cl.' | 識別記号 | FI | テーマコード(参考) |
|---|---|---|---|
| H04L 12/58 | | H04L 11/20 | 101Z |

(72)発明者 川村 亨
東京都武蔵野市御殿山一丁目１番３号 エヌ・ティ・ティ・アドバンステクノロジ株式会社内
(72)発明者 鶴巻 宏治
神奈川県横浜市中区不老町二丁目９番１号 エヌ・ティ・ティ・インテリジェントテクノロジ株式会社内

Fターム(参考) 5B049 BB11 CC05 EE03 FF03 FF04 GG04 GG07 GG10
5B089 HA10 JA08 JA33 JB23 KA17 KB13 KC57 KC58 KH30
5J104 AA07 AA16 EA04 EA24 EA25 EA26 KA01 KA03 KA06 KA07 KA10 KA21 NA03 NA05 NA11 PA07 PA10
5K030 GA15 HA07 HC01 JT03 LD19